The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
7/18/2012

SUBJECT:
Multiple Vulnerabilities in Mozilla Products Could Allow Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Mozilla Firefox, Thunderbird, and SeaMonkey applications, which could allow remote code execution. Mozilla Firefox is a web browser used to access the Internet. Mozilla Thunderbird is an email client. Mozilla SeaMonkey is a cross platform Internet suite of tools ranging from a web browser to an email client. Successful exploitation of these vulnerabilities could result in either an attacker gaining the same privileges as the logged on user, or gaining session authentication credentials. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- Firefox versions prior to 14
- Thunderbird versions prior to 14
- SeaMonkey versions prior to 2.11

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:
Multiple vulnerabilities have been discovered in Mozilla Firefox, Thunderbird, and SeaMonkey. The details of these vulnerabilities are as follows:

Miscellaneous memory safety hazards (MFSA 2012-42)
Two memory corruption vulnerabilities exist in Mozilla products. Successful exploitation could result in remote code execution. Failed attacks may result in a denial of service condition. (CVE-2012-1949) (CVE-2012-1948)

Incorrect URL displayed in address bar through drag and drop (MFSA 2012-43)
By dragging and dropping the address bar onto a page, the page load cancels. This causes the address of the previous site entered to be displayed in the address bar instead of the currently loaded page. This could lead to potential phishing attacks on users. (CVE-2012-1950)

Gecko memory corruption (MFSA 2012-44)
Four memory corruption vulnerabilities exist in Mozilla products. There are two use-after-free problems, one out of bounds read bug error, and a bad cast issue. The first use-after-free problem is caused when an

array of nsSMILTimeValueSpec objects is destroyed but attempts are made to call into objects in this array later. The second use-after-free problem is in nsDocument::AdoptNode when it adopts into an empty document and then adopts into another document, emptying the first one. The heap buffer overflow is in ElementAnimations when data is read off of the end of an array and then pointers are dereferenced. The bad cast happens when nsTableFrame::InsertFrames is called with frames in aFrameList that are a mix of row group frames and column group frames. AppendFrames is not able to handle this mix. Successful exploitation could result in remote code execution. Failed attacks may result in a denial of service condition. (CVE-2012-1951) (CVE-2012-1952) (CVE-2012-1953) (CVE-2012-1954)

Spoofing issue with location (MFSA 2012-45)
By calling history.forward and history.back an attacker can displaying the previous site in the address bar but change the baseURI to the newer site. This can be used for phishing by allowing the user input form or other data on the newer, attacking, site while appearing to be on the older, displayed site. (CVE-2012-1955)

XSS through data: URLs (MFSA 2012-46)
A Cross-Site Scripting vulnerability has been reported in the context menu by using a data: URL. The context menu functionality allows "View Image", "Show only this frame", and "View background image" which could lead to Cross-Site Scripting attacks. (CVE-2012-1966)

Improper filtering of JavaScript in HTML feed-view (MFSA 2012-47)
JavaScript can be executed in the HTML feed-view using the <embed> tag within the RSS <description>. This is because the <embed> tag is not filtered out during parsing. Successful exploitation could result in Cross-Site Scripting attacks. (CVE-2012-1957)

use-after-free in nsGlobalWindow::PageHidden (MFSA 2012-48)
A use-after-free error in nsGlobalWindow::PageHidden is caused when mFocusedContent is released and old FocusedContent is used afterwards. Successful exploitation could result in remote code execution. Failed attacks may result in a denial of service condition. (CVE-2012-1958)

Same-compartment Security Wrappers can be bypassed (MFSA 2012-49)
A security bypass vulnerability exists in Same-Compartment Security Wrappers (SCSW) by passing them into another compartment. Some other compartments strip off the SCSW before processing, which results in the bypassing of SCSW. This could result in un-trusted content having access to the Extensible Bindings Language (XBL). (CVE-2012-1959)

Out of Bounds Read in QCMS (MFSA 2012-50)
An out of bounds read exception was reported in QCMS, Mozilla's color management library. A specially crafted color profile could allow a portion of a user's memory to be incorporated into an image and possibly deciphered. Successful exploitation could result in attacker being able to read sensitive data from memory. (CVE-2012-1960)

X-Frame-Options header ignored when duplicated (MFSA 2012-51)
A security bypass vulnerability exists in the X-Frame-Options header. The X-Frame-Options response header is used to prevent Click-jacking attacks by making sure their content is not embedded in other sites. The X-Frame-Options header is ignored when the value is duplicated, for example"X-Frame-Options: SAMEORIGIN, SAMEORIGIN". Successful exploitation could result in users not being protected against Clickjacking attacks.(CVE-2012-1961)

JSDependentString::undepend string conversion results in memory corruption (MFSA 2012-52)

A memory corruption vulnerability exists in the way JSDependentString::undepend changes a dependent string into a fixed string. When the "*undepend*" occurs, the base data is freed and leaves other dependent strings with dangling pointers. Successful exploitation could result in remote code execution. Failed attacks may result in a denial of service condition. (CVE-2012-1962)

Content Security Policy 1.0 Implementation Errors Cause Data Leakage (MFSA 2012-53)
Content Security Policy is an added layer of security that helps to detect and mitigate certain types of Cross-Site Scripting and Data Injection attacks. CSP violation reports generated by Firefox and sent to the "report-uri" location include sensitive data in the "blocked-uri" parameter. This data can be used to retrieve a user's OAuth 2.0 access tokens and OpenID credentials. (CVE-2012-1963)

Clickjacking of Certificate Warning Page (MFSA 2012-54)
A man-in-the-middle attacker can use an iframe to display a fake certificate error warning message with the "Add Exception" button of a real warning page from another site. Successful exploitation could result in the user inadvertently adding a security exception for an undesired host. (CVE-2012-1964)

Feed: URLs with an innerURI Inherit Security Context of Page (MFSA 2012-55)
It has been reported that Mozilla allows the pseudo-protocol feed: to prefix any valid URL. Since this is possible, JavaScript URLs that execute scripts can be used in the context of the feed: protocol to contribute to Cross-Site Scripting attacks. Successful exploitation could result in remote code execution. (CVE-2012-1965)

Code Execution Through JavaScript: URLs (MFSA 2012-56)
An arbitrary code execution vulnerability has been discovered in the Gecko engine, which is included in Firefox, Thunderbird, and SeaMonkey products. The engine uses a JavaScript sandbox to only allow scripts to run in the context of a web page. Sometimes, JavaScript: URLs executed in the sandbox can escape the sandbox environment and run with elevated privileges. Successful exploitation could result in remote code execution. Failed attacks may result in a denial of service condition. (CVE-2012-1967)

RECOMMENDATIONS:
The following actions should be taken:

- Upgrade vulnerable Mozilla products immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Do not open email attachments or click on URLs from unknown or untrusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Mozilla:
http://www.mozilla.org/security/announce/

SecurityFocus:
http://www.securityfocus.com/bid/54572
http://www.securityfocus.com/bid/54573
http://www.securityfocus.com/bid/54574
http://www.securityfocus.com/bid/54575
http://www.securityfocus.com/bid/54576
http://www.securityfocus.com/bid/54577
http://www.securityfocus.com/bid/54578

http://www.securityfocus.com/bid/54579
http://www.securityfocus.com/bid/54580
http://www.securityfocus.com/bid/54581
http://www.securityfocus.com/bid/54582
http://www.securityfocus.com/bid/54583
http://www.securityfocus.com/bid/54584
http://www.securityfocus.com/bid/54585
http://www.securityfocus.com/bid/54586

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1948
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1949
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1950
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1951
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1952
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1953
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1954
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1955
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1956
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1957
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1958
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1959
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1960
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1961
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1962
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1963
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1964
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1965
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1966
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1967